MEMORANDUM OF LAW

Plaintiff objects to all of the MC's rulings in the RR, believing the reasoning used is flawed *ab ovo usque ad malain* – or at least in all of the following ways; (1) the RR wrongly opposes congressional intent in its construing of the Wiretap Act, and (2) the RR runs afoul of technical realities related to computer hardware and the delivery mechanisms running the internet, and (3) The RR runs counter to more more technically and constitutionally sound judicial interpretations of what comprises an "intercept." Perhaps most unfortunate of all, the RR is also (4) dangerously counter to our already battered privacy interests in this ever-changing Digital Age.[1]

Introduction

Forty years ago, this Circuit found that the federal Wiretap Act "establishes abroad prohibition on all private electronic surveillance and that a principal area of congressional concern was electronic surveillance for the purposes of marital litigation." *United States v. Jones,* 542 F.2d 661, 669 (6th Cir. 1976); see also *id.* At 667 (quoting Senate Report's statement of Wiretap Act's purpose as addressing the "tremendous scientific and technological developments that have . . . made possible today the widespread use and abuse of electronic surveillance techniques"). This case presents *Jones's* logical extension to the Internet age, in which Awareness Technologies intentionally intercepts and discloses private electronic communications for its commercial gain through WebWatcher, software it designed to help its customers catch a cheating spouse. As this Court recognized, in such circumstances, "it is not just the privacy of the targeted spouse which is being violated, but that of the other party to the conversation as well." *Id.* at 670. Here, Tech's acts represent violations of the federal and Ohio Wiretap Acts and Ohio common law . Tech acquired Plaintiff's private communications contemporaneously –or close enough therein- with their transmission as defined by district courts within the

[1] This issues herein have been argued many times in the five years the case has been in this forum. Although plaintiff again incorporates those arguments by reference, it is perhaps wise to also *directly* reference and re-argued those points herein. As such, many of these arguments will cite to plaintiff's own previously submitted documents containing those arguments–both in this forum and in his prior appeal.

Sixth Circuit and other Courts of Appeals. Awareness also violated 18 U.S.C. § 2512 when a manufacturer knowingly designs a product primarily useful for interception of private communications.

Much to its credit, a few years ago the Magistrate Court (or "MC") impressively rejected decades of improper reasoning as to a critical issue within the Wiretap Act, while suggesting that "a rethinking of the definition of the 'contemporaneous' standard of intercept might be necessary and that the timing of the intercepted data's transmission should be irrelevant, allowing the ECPA to be applied." Gariella E. Bensur, *Cover your Webcam: e ECPA's Lack of Protection against Software That Could Be Watching You*, 100 Cornell L. Rev. 1191 (2015)[2].

Apparently something has since changed that is not really explained by the fact that the appellate court adopted the contemporaneous standard, nor by the different standards applies to this new stage of this lawsuit. Fast forward almost a half a dozen years, and now we find this same Magistrate Court advocating and recommending the complete opposite of what it recommended in 2013; that this Circuit be guided by the *absolute most* dangerous and regressively narrow interpretation of the recently adopted "contemporaneous" standard of intercept. An abysmal and likely soon to be extinct interpretation as to what comprises an "intercept" under the Wiretap Act ("the Act" or "ECPA"). Moreover, the Magistrate Court has sided with circuits that have (plaintiff believes) improperly removed transient temporary storage necessary to the transmission of data from type of communications the Wiretap Act was meant to protect. No matter, whether it likes it or not, the Magistrate Court got it right the first time around and so the District Court should now wisely reject the recent RR in its entirety.[3]

---

[2] referring to *Luis v. Zang*, No. 1:11-cv-884, 2013 WL 811816 at *6–7 (S.D. Ohio Mar. 5, 2013). Available at: http://scholarship.law.cornell.edu/clr/vol100/iss5/4

[3] While nothing in this objection will change a thing in the lower forum, rights must be preserved on appeal and thus the submission of this lengthy document. Much of this objection has been copied and pasted from previous submissions that went fully unacknowledged and un-responded to by either of the courts in the the lower forum in the five years the case has remained here. Since nothing has truly changed in this case from the time those documents were submitted many years ago, it would seem proper and more efficient that Plaintiff simply incorporate those documents here by reference and incorporate those arguments herein. However, as evidenced in the MC's recent Order, many courts apparently disfavor such wide-scale use of argument incorporation. Nonetheless Plaintiff incorporates all relevant arguments made during this case. Most of those are located within six particular documents in the lower forum (Doc. #'s 91, 97, 118 and 222 in the 629 case and Doc. #'s 101 and 175 in the 884 case) and those argued in appeals (Document # 7, 13, 26, 35 and 43). While all the earlier arguments are adopted by

This memorandum will advocate for the correct application of Congress' intentions when it authored the Wiretap Act, which run parallel (and should simultaneously serve) to Plaintiff's objections of the many errors made by the Magistrate Court which – in keeping with its five year track record – again utilized improper reasoning and myopic vision in reaching a conclusion that undermines our privacy rights in the digital age and led to an absurd result.

ARGUMENT

I. The Magistrate Court Erred Throughout Its Report and Throughout This Entire Case

Plaintiff believes the Magistrate Court erred in at least the following ways within its RR; (1) by refusing to consider amended documents prior to issuance of her RR that pointed out specific facts in evidence that present issues at trial,[4] (2) by not recognizing that even without acceptance of the amendments, there is plenty of evidence in the record that Awareness intercepted, disclosed, and intentionally used Plaintiffs Electronic Communications, (3) with its tentative suggestion/partial recommendation that plaintiff might lack lack standing to bring an invasion of privacy claim under Ohio Law, and (4) by finding that Awareness is entitled to Judgment on the §2511 claims based upon the lack of any 'intercept' of his 'electronic communications' while still 'in flight,' based in part by (a) the MC's improper interpretation standards, and (b) its ignoring the fact that the definition of "in flight" and "intercept" are not clear or universally defined by the circuit courts, and (c) its refusal to recognize that volatile/temporary memory is not the "permanent storage" intended to apply to the SCA instead of the Act, and (d) ignoring the fact that all parts of a communication- including what is found in the RAM- was also meant to be protected by the Act, and (6) by overlooking the critical importance of the type of acquisition involved in this case; i.e. *continuous surveillance* by *automatic*

---

reference herein, they will be re-argued here again as a precaution. Any relevant arguments mistakenly omitted should nonetheless be considered already argued and properly objected to for appeals.

[4] The MC's rejection of those submissions was recently objected to in Docs. # 226 and 227, which have yet to be ruled on by this Court. Those arguments also contributed to the errors objected to in the RR. While referencing by incorporation is typically disfavored, those objections have yet to be ruled upon and so in the interest of judicial economy, it is best they be incorporated herein, rather than relisting and re-arguing them here again. Therefore, those documents are incorporated herein as if argued anew.

routing software, and (7) attaching no relevance to the undisputed fact that Tech engaged in the violation during a protracted period of time, and (8) with its ruling that Tech is entitled to judgment on the Ohio Wiretap Law Claim, and (9) ruling that Tech is entitled to judgment on breach of privacy claim, having partially based her reasoning on irrelevant matters having to do with (a) the licensing agreement, (b) the lack of evidence that the intrusion was "wrongful," or perhaps not wrongful *enough* to satisfy state standards (c) the allegedly private subject matter of the intrusion, having apparently found the messages were not so private as to deserve extra protection (when in fact the messages were so private they likely doomed her divorce case, and (d) with its findings about Plaintiff's supposed lowered expectations of privacy due to its incomplete and erroneous findings that married people have a lowered expectation of privacy within their digital world, and (10) by its continued use of cases that have little to nothing to do with the unique circumstances in this case, and that indeed sometimes support this case more than help defeat it.

If upheld as is, the MC's ruling will reward and encourage continued and expanded abuses of the multiple loopholes in the ECPA that have been noted and criticized since the advent of the Internet and advanced spyware in the mid to late 1990's. In order to prevent being on the wrong side of history in this important arena of privacy, Plaintiff believes this Court should do the following[5]; A) reject the RR while adopting a broader approach to what comprises an "intercept" under the Wiretap Act – one more in line with that evidenced by the 1st and 7th circuits (as well as similar rulings in various district courts) and, B) rule that the definition of "intercept" should also include any acquisitions while instant messages, digital communications of any kind, and e-mails are in temporary storage, and C) rule that this Plaintiff has standing because a competent jury could find from the evidence already submitted (by both parties as well as those in the previously connected case) that Plaintiff's case meets those requirements as ruled in those circuits.

Tech's business is spying on private conversations through its software, WebWatcher. WebWatcher records everything that happens on a monitored computer: keystrokes, emails, instant messages, and more. All

[5] Ideally, the District Court will adopt or at least advocate a different standard altogether – the more advanced, constitutionally and technically sound "router switching" analysis used by the Court in *Klumb v. Goan*, 2012 U.S. Dist. LEXIS 100836 (E.D. Tenn. 2012). Nonetheless, Plaintiff realizes such a request is likely just another "bridge too far" for this Court at this point.

that WebWatcher records is kept on Tech's servers to be accessed by Tech's customers through Tech's Internet site. Plaintiff is a victim of Tech's spying. When one of Tech's customers bought and used WebWatcher to record his wife's Internet activity, Tech captured Plaintiff's communications as well. Plaintiff's claims under the federal Wiretap Act § 2511 and the Ohio Wiretap Act should not be dismissed because Tech intentionally intercepted his electronic communications. Previously in 2013, the Magistrate Judge correctly determined that WebWatcher intercepted Plaintiff's communications in its Report and recommendations (Doc. #109) but in its most recent Report due to the MC's inexplicable embrace of the absolute most narrow interpretation of the contemporaneous standard possible, leading to its improper conclusion that no intercept has occurred. The MC has either ignored altogether, or misunderstood and misapplied the contemporaneous standard as has been applied by more recent Circuit court decisions. In fact the MC could have allowed this case to continue onto trial, and yet remained well within the boundaries of the contemporaneous standard– it just chose not to do so.

As part of WebWatcher's design, Tech maintains an Internet-based platform to keep all of the communications WebWatcher records. Because WebWatcher has been certified by Tech as copying only form the RAM, it means it copies the information in milliseconds, which is practically in real time (See Exhibits on Ram) then some seconds later sends the acquired information to Tech's servers for later access by its customers, it is Tech that intercepts the communications. The time it copies is what's important, not when it sends to its servers. By design, Tech is an informant, providing secretly intercepted information to WebWatcher's users for a fee. When its customers access that information is not relevant to Tech's interception. Second, through § 2520(a), the Wiretap Act provides a right of action for any violation of its provisions as long as a plaintiff falls into the narrow category of those who have suffered harm. Section 2520 operates in two parts. First, it requires that a plaintiff's communications have been intercepted, disclosed, or used in violation of the Act. A plaintiff so harmed may sue a defendant who engaged in violating the Act. Congress intentionally used broader language to define the class of defendants than it did in identifying proper plaintiffs. A manufacturer engages in the violation that caused the plaintiff's harm when there is a nexus between the manufacture of the product and the interception. Such a nexus exists when a manufacturer knows

its device is primarily useful for intercepting communications and its product is used according to that design. Plaintiff has standing because his communications were intercepted and or acquired (acquisition was never challenged or disputed by Tech), used and delivered by a manufacturer that sold software that it knew was primarily useful for interception (establishing a violation of § 2512). Plaintiff then connected these two—showing that Tech engaged in the violation that caused his harm—by pleading that the software Tech made was used to intercept or at least acquire, use and deliver his communications. Similar manufacturer liability has been recognized by the Supreme Court in the copyright context in *Metro-Goldwyn-Mayer Studios Inc., v. Grokster, Ltd.,* 545 U.S. 912 (2005), through reasoning that applies with equal force to the Wiretap Act. Cases that have found no private claim under § 2512 rely on language or logic rooted in superseded statutory language. As such, the cases finding no private right of action are unreliable. Even in courts that prohibit recovery for violations of §2512 alone, many allow liability "in the presence of intercept, use or delivery." *See e.g. See e.g. DirecTV, Inc. v.Moreno, 2003 WL 22927883 (D.N.J.)* at *2. Moreover, when statutes are written in the disjunctive, a party needs prove only one of the factors to meet the statutory requirement. West's A.I.C. 35-33.5-5-4(a); *See also Dommer v. Dommer,* 829 N.E.2d 125 (Ind. Ct. App. 2005)(because phrase "intercepted, disclosed, or used," was written in the disjunctive, plaintiff needed to allege that only one of those three violations occurred.). under common law invasion of privacy claim under Ohio law. Tech's repeated captures of his personal communications without his knowledge or consent intruded into the sanctity of his private life in a manner offensive to any reasonable person

A. Plaintiff Does Not Lack Standing to bring any civil claim under 18 U.S.C. § 2520 or to Bring an Invasion of Privacy claim under Ohio Law

The MC seemed to indicate Plaintiff might have standing, though she seems to have stopped short of ruling on the matter as the "issue of standing has not been briefed." Nonetheless, Plaintiff does not lack standing. He met Ms. Zang through the Internet and "commenced daily communications with her from his home. These daily private communications consisting of "thousands" of "AOL instant messages" and emails over a month or more were intercepted, or actually acquired and used and delivered in real time (or close enough thereof) by Tech without Mr. his knowledge or consent. Moreover, Tech's "monitoring" of "anything

typed in real time" along with the storage, summarization, processing and delivery of these communications served no public aim — indeed, its purpose was to disturb Plaintiff's private rights. Such monitoring was as invasive as the reading of personal emails in *Lazette* if not worse, as Plaintiff could never have consented to (or had reason to believe) his communications were being monitored. To Tech, Plaintiff was mere collateral damage of the wrongful acts of others using the product they designed, marketed and used for surreptitious monitoring of electronic communications yet Plaintiff's private life would have remained private but for Tech's intentional interception of his communications

Ohio recognizes the tort of invasion of privacy when a plaintiff's private activities are intruded upon "in such a manner as to outrage . . . a person of ordinary sensibilities." *Sustin v. Fee*, 431 N.E.2d 992, 993–94 (Ohio 1982); *Housh v. Peth*, 133 N.E.2d 340, 343–44 (Ohio 1956). While Ohio requires more than mere indignities to satisfy the tort, *Yeager v. Local Union 20, Teamsters, Chauffeurs, Warehousemen & Helpers of America*, 453 N.E.2d 666, 671–72 (Ohio 1983) *abrogated on other grounds by Welling*, 866 N.E.2d at 1059, Ohio law does not set an unattainable bar; repeated efforts to obtain information by a party, even without malice, can suffice. *Welling*, 866 N.E.2d at 1057–59; *see Charvat v. NMP, LLC*, 656 F.3d 440, 452–54 (6th Cir. 2011) (applying Ohio law to conclude that thirty-three unsolicited telephone calls over a three-month period constituted an invasion of privacy given the strong interests preserving the sanctity of one's home).

The most commonly pursued claim is for intrusion. *See, e.g.*, *Housh*, 133 N.E.2d at 343. To succeed, a plaintiff must allege that a wrongful intrusion into a private place occurred in a manner offensive to a reasonable person. *Id.* at 344; *see also Steffen v. Gen. Tel. Co.*, 395 N.E.2d 1346, 1349 (Ohio Ct. App. 1978). "The intrusion alone is enough so long as it goes to a truly private matter and is of a

nature to cause mental suffering or humiliation to a person of ordinary sensibilities." *Steffen*, 395 N.E.2d at 1349.

In weighing offensiveness, courts evaluate the "totality of the circumstances," which encompasses the nature of the interference, the individual's private rights, and the public's interest in the intrusion. *Kohler*

v. City of Wapakoneta, 381 F. Supp. 2d 692, 703–04 (N.D. Ohio 2005) (citing *Housh*, 133 N.E.2d at 343). But when determining an intrusion's wrongfulness, the court need only evaluate how the intrusion was made to determine if it exceeded the bounds of reasonable behavior. *See Kohler*, 381 F. Supp. 2d at 704; *Strutner v. Dispatch Printing Co.*, 442 N.E.2d 129, 132 (Ohio Ct. App. 1982) ("'Wrongful' does not require that the intrusion itself be wrongful in the sense that there is no right to make any intrusion. Rather, 'wrongful' may relate to the manner of the making of the intrusion . . . ."). This is because the injury is not rooted in the intruder's procuring information, but rather in protecting "the person's interest in solitude or seclusion" from "intentional interference." *Kohler*, 381 F. Supp. 2d at 704.

Intercepting private communications such as emails and IMs constitutes an invasion of privacy under Ohio law. *Lazette v. Kulmatycki*, 949 F. Supp. 2d 748, 760–61 (N.D. Ohio 2013). The plaintiff in *Lazette* claimed invasion of privacy by a co-worker who accessed her private email account without permission. *Id*. The court found that the plaintiff reasonably expected that no one would access her

email account, "particularly in light of her unawareness of [the defendant's] ability to do so." *Id*. The court found the plaintiff's emails "highly personal and private" and that a reasonable jury could find the defendant's reading of "tens of thousands of such private communications . . . highly offensive." *Id*.

Plaintiff adequately pleaded an invasion of privacy by Awareness, having met Ms. Zang through the Internet and "commenced daily communications with her from his home." (Appeals Doc . 39, Compl. ¶ 19, PageID # 314.) These daily private communications constituting "thousands" of "AOL instant messages" and emails over more than a month Awareness without his knowledge or consent. These repeated interceptions (thousands of which are in evidence as intercepted instant messages, each of which is considered an intercept) exceeded the mere double-digit volume of communications found to be intrusive in *Charvat*. Moreover, Tech's "monitoring" of "anything typed in real time" which Tech never actually denied (they just insist it is not contemporaneous, but it is still considered "real time" if only for marketing purposes) along with the storage and processing of these communications served no public aim; indeed, its purpose was to

disturb Plaintiff's private rights. Such monitoring was as invasive as the reading of personal emails in *Lazette* if not worse, as Plaintiff could never have consented to (or had reason to believe) his communications were being monitored. To Awareness, Plaintiff may be mere collateral damage of the wrongful acts of others; yet his private life would have remained private but for Awareness's intentional interception of his communications.

B. Tech is Not Entitled to Judgment on Plaintiff's §2512 Claim

Awareness remains entitled to judgment as a matter of law on Plaintiff's alternate theories that the Defendant "intentionally disclose[d]…the contents of any…electronic communication, knowing or having reason to know that the information was obtained through the interception of …electronic communication," or that Defendant "use[d]" the contents of information "obtained through the interception of…electronic communication." Id.

C. Tech Knew Or Had Reason To Know That It Illegally Intercepted And Disclosed Plaintiff's Communications In A Way That Would Be Offensive To A Reasonable Person In Violation Of Ohio Law.

Awareness's arguments against Plaintiff's Ohio law claims are similarly unavailing. As set out in his opening brief, Plaintiff specifically alleged that Tech previously argued that "Luis' attempt to place the burden on Awareness Technologies to determine whether any communications that may have been place [sic] in storage through the use of Awareness Technologies software is improper" because "the burden is not on Awareness Technologies to review all stored communications through the use of its software to determine whether they were legally acquired." (AT Br. at 18–19.) However, this Court recognizes that Ohio's wiretap law outlaws the use and disclosure of intercepted communications "when a person acts 'knowing or having reason to know' that the information was obtained illegally." Nix v. O'Malley, 160 F.3d 343, 348 (6th Cir. 1998). Even if Awareness had no specific knowledge that it was distributing illegally intercepted electronic communications, Tech had reason to know because of how it marketed WebWatcher. This is enough under Ohio law. Ostensibly legal uses of WebWatcher—monitoring of children and employees with their consent—

cannot whitewash the foreseeable (and encouraged) illegal uses of the program. Nowhere in WebWatcher's marketing materials is there mention of obtaining the monitored person's consent.

Moreover, even if Awareness lacked personal knowledge about its software's misuse, the Magistrate Judge erred in requiring this mental state. (R. 109, R.&R., PageID # 764.) Ohio law requires only that Awareness purposely use data that it had reason to know was wrongly acquired. Awareness's purposeful use of the data it acquired is essential to the viability of its product. Moreover, Awareness's advertisements presented sufficient circumstantial evidence to illustrate that Awareness had reason to know customers used its software in a manner that violated state privacy laws. Awareness advertised its software to intercept a cheating spouse's communications and, by extension, those of anyone with whom the spouse communicated. (R. 91-1, Resp. in Opp'n to Mot. to Dismiss, Pl.'s Ex. C–E, PageID ## 675–77.) Because it strains credibility to think cheating spouses would consent to having their conversations monitored, it is reasonable to infer Awareness had reason to know that it disclosed communications illegally obtained by its software.

Further, because Awareness had not "reviewed any of the alleged communications that are referenced in the Complaint," it could not conclude that its interceptions were gathered lawfully before disclosure to its clients. (R. 77-1, Mot. to Dismiss, Miller Aff. ¶ 8, PageID # 538.) Thus, Awareness could not lawfully disseminate Plaintiff's conversations because it could not know if they were lawfully acquired.

II. Plaintiff's Claim Against Awareness For Intercepting and Disseminating His Electronic Communications Satisfies The Elements Of Ohio's Wiretap Act.

Plaintiff's Ohio Wiretap Act claim is properly pleaded because the state cause of action is even broader than the federal statute as follows;

O.R.C. §§ 2933.52(A)(1)

(3) ("No person purposely shall . . . intercept a wire, oral, or electronic communication . . . ; Use, or attempt to use, the contents of a wire, oral, or electronic communication, knowing or having reason to know that the contents were obtained through the interception . . . ."). Like the federal statute, Ohio folds corporate entities into its definition of "person," placing firms like Awareness within the scope of the principle civil cause of action when they unlawfully intercept private communications. §§ 2933.51(K), 2933.52(A); *see State v. Bidinost*, 644 N.E.2d 318, 329–30 (Ohio 1994) (discussing the broader scope of Ohio's Wiretap Act, while

also recognizing its consistencies with the federal statute). Concurrently, while Ohio's statute parallels the federal definition of interception, its prohibition on "use" also extends to disclosure of communications.*See Nix v. O'Malley*, 160 F.3d 343, 350 (6th Cir. 1998). *Compare* 18 U.S.C. § 2511(c)–(d), *with* O.R.C. § 2933.52(A)(2)–(3). Thus, § 2933.52(B) forbids corporations from intercepting, disclosing, or disseminating private conversations subjecting them to civil penalties for doing so. *Nix*, 160 F.3d at 350 (permitting property developer to proceed to jury trial where entity disclosed contents from recordings of developer's cordless telephone calls).

Thus, under Ohio law, an aggrieved person may bring an action for damages against a company for either (1) intercepting an "electronic communication" or (2) for disclosing the contents of an electronic communication, when the company would have "reason to know" the contents were illegally intercepted. O.R.C. §§ 2933.51–.52; *Nix*, 160 F.3d at 348–50. "[T]he trier of fact may rely on circumstantial evidence to prove 'reason to know.' " *Nix*, 160 F.3d at 349; *accord United States v. Wuliger*, 981 F.2d 1497, 1502 (6th Cir. 1992) (concluding that "reason to know" requires that a seller have her eyes open "to the objective realities of the sale").

Here, the Magistrate Judge wrongly dismissed the Ohio Wiretap Act claim by assuming that Plaintiff pleaded only manufacturer liability. (R. 109, R.&R., PageID # 761.) As under federal law, Plaintiff pleaded direct claims against Awareness for its interception and disclosure of his communications. (R. 39, Compl. ¶ 107, PageID # 335.) Plaintiff's allegations also showed that Awareness used the intercepted data by maintaining it online, processing user "alert words," and disclosing to its clients the contents of intercepted communications. (R. 39, Compl., Pl.'s Exs. C–D1, PageID ## 349–50); (R. 91-1, Resp. in Opp'n to Mot. to Dismiss, Pl.'s Ex. B, PageID # 674.)

Interceptions Of His Communications State Causes Of Action Under The Different Standards Of Ohio Law.

The Magistrate Judge dismissed Plaintiff's claim under the Ohio Wiretap Act "for the same reasons" that she found no manufacturer liability under the federal statute—"the statute does not contemplate imposing civil liability on software manufacturers and distributers for the activities of third parties." (R. 109, R.&R., PageID # 763.) First, this conclusion fails to consider that Awareness itself intercepted Plaintiff's communications, making it directly liable under the Ohio statute as under § 2511. Plaintiff's state law claims,

like his federal claims, are made against Awareness for "intercept[ing] the communications live as [they were] being written" and "rout[ing] the intercepted communications to [its] servers located in California to be stored." (R. 39, Compl. ¶¶ 77, 96, PageID ## 327, 331.) The Magistrate Judge erred in not recognizing this as a direct cause of action for interceptions and disclosures made by Awareness. Further, Plaintiff's allegations support a claim that Awareness "used" Plaintiff's communications by disclosing them, having reason to know that the contents were obtained by illegal interception. Ohio Rev. Code § 2933.52(A)(3) (2015).

Second, the Magistrate Judge erred in dismissing all of Plaintiff's tort claims based upon his statement in opposition to Awareness's Motion to Dismiss that "only discovery can disclose the necessary facts relating to the extent of

Awareness's guilt and liability." (R. 91, Opp'n to Mot. to Dismiss, PageID # 670.) The Magistrate Judge found that, because Plaintiff had not alleged that Awareness "had any personal knowledge of [the] intended use of its WebWatcher product" or "that Awareness had any agreement . . . to intercept Plaintiff's communications," Plaintiff had alleged no facts to state an invasion of privacy claim. (R. 109, R.&R., PageID # 764.) Alleging Awareness had "personal knowledge" of or an "agreement" relating to the wrongdoing is not necessary for all of Plaintiff's common law claims. (*Id.*, PageID # 764.) Plaintiff's complaint alleged that "more than 270 days of illegally intercepted electronic communications . . . w[ere] permanently recorded on [Awareness]'s servers" in spite of "an objectively reasonable expectation of privacy in the conversations," and attached the exhibits illustrated how WebWatcher intercepted his information. (R. 39, Compl. ¶¶ 73, 101, PageID ## 326, 333; *Id*. at Pl.'s Exs. D–D3, PageID ## 350–52.) Thus, Plaintiff adequately pleaded Ohio Wiretap Act and invasion of privacy claims because (contrary to the Magistrate Judge's assertion) allegations of personal knowledge or an agreement are not needed for these causes of action. (R. 109, R.&R., PageID # 764.)

The Magistrate Court's severely narrow interpretation of the contemporaneous standard is improper, clashes with this Circuit's Own Landmark Privacy Decisions While Embracing Outdated and Disfavored and Absurd Case Law

As if to emphasize the South's longing to make domestic violence great again, one of the worst decisions ever made by an actual circuit court was aimed at the Wiretap Act's intended new protections for abused and controlled spouses. That case was *Simpson v. Simpson*. 490 F.2d 803 (5th Cir.), cert. denied, 489 U.S. 897 (1974), one of the most myopic, and unlovable rulings ever to come out of any actual circuit court perhaps the 1920's.6 Despite a mountain of evidence at its disposal and unimpeachable testimony from the most credible sources available who testified that Title III *did* apply to electronic surveillance between spouses, the *Simpson* Court inexplicably found that Congress did not intend title III to apply to domestic conflicts in a home. [7] Incredibly, other courts soon began to look to *Simpson* for guidance in interpreting that Act's provisions and *Simpson* was well on its way towards becoming the sentinel Wiretap Act case concerning the legality of domestic surveillance in domestic situations. Thankfully, that regressive, offensive and hard fisted decision came to a mercifully quick end soon after the Sixth Circuit ruled in *United States v. Jones*, 542 F.2d 661 (6th Cir. 1976). In *Jones*, the Sixth Circuit found that § 2511(1)(a) *was* intended to apply to interspousal wiretaps, noting that the legislative history left "no doubt that the Act was intended to reach private electronic surveillance…and that Congress was aware that a major area of use for surveillance techniques was the preparation of domestic relations cases" *Jones* 542 F.2d 661 *24.[8] The Sixth Circuit Court determined the Simpson view to be "untenable" because it "contradicts both the explicit language of the statute and the clear intent of Congress expressed in the Act's legislative. Yet Regardless of that unsavory back history, in its RRR the MC Court seems almost wistful of those days, seeming to be advocating for that horrid decision while attempting to advocate for her untenable one.

---

[6] One prime example of the *Simpson* Court's disconnect with proper jurisprudence is evidenced in the fact that the Court ignored the testimony of the two of the primary authors of the Wiretap Act, G. Robert Blakey, and senator Roman Hruska's who stated that in Title III "A broad prohibition is imposed on private use of electronic surveillance, particularly in domestic relations..." Instead the court found the words of a "private investigator" much more compelling—actually quoting him in its ruling as follows; "…in any domestic squabble, there is a 50% better chance of a couple being reconciled. Every time we make a case, I practically feel like a surgeon who is cutting out a cancer." *Simpson*, 490 F.2d at 808 n.14.

[7] One prime example of the *Simpson* Court's disconnect with proper jurisprudence is evidenced in the fact that the Court ignored the testimony of the two of the primary authors of the Wiretap Act, G. Robert Blakey, and senator Roman Hruska's who stated that in Title III "A broad prohibition is imposed on private use of electronic surveillance, particularly in domestic relations..." Instead the court found the words of a "private investigator" much more compelling—actually quoting him in its ruling as follows; "…in any domestic squabble, there is a 50% better chance of a couple being reconciled. Every time we make a case, I practically feel like a surgeon who is cutting out a cancer." *Simpson*, 490 F.2d at 808 n.14.

[8] *See more,* S.Rep. No. 1097, reprinted in 2 U.S.Code Cong. & Admin.News 1968, 90th Cong., 2d Sess., at p. 2113. *See also id* at pp. 2153, 2156, 2180-81

The MC has now again issued that same industry a renewed license to continue to freely intercept all of our communications with little fear of legal ramifications or since the industry's worst violator of the Act has been let free in a privacy case in the continuing emasculation of the vital second prong of the Act (civil ECPA) that Congress intended to specifically *deter* the growth of private sector industries of intercept?[9] The *Jones* Court knew what it meant to victims of domestic abuse if *Simpson* came to establish itself as the dominant case law of the land concerning the Wiretap Act, and the tone of its ruling leaves little doubt as to how the Jones Court felt about the reasoning used by the *Simpson* Court. And yet despite that notable decision, , here we are again in in a case spawned from the ashes of a brutal domestic case where exactly what the *Jones* Court feared in the 70s has been allowed to become a terrifying staple of the modern day divorce for more than a decade now. [EXHIBIT or footnote]. In fact, the problem is much worse than what was possible in the 70's since spyware's web-based capabilities has enabled a type of stalking and control over its victims that phone recordings could never have provided their users. Web Watcher is a prime example of the evolution of a technology that has morphed from a relatively simple locally based keylogger into a destructive tool of domestic warfare.

The *Simpson* ruling was so disfavored that it was overwhelmingly rejected by most of the nation's courts soon after *Jones*, and was eventually overturned almost three decades later. [10]

---

[9] With this Circuit's unique history concerning the 4th Amendment, it defies imagination that such a ruling would be allowed to stand. Particularly when one considers how the impressive stand this Circuit's predecessor Court took against one of the first major judicial assaults on the Wiretap Act's privacy protections. The 5th Circuit's ruling would surely have crippled the Act's intended protections ways back in the mid-seventies. have crippled the Act as far back as 1974. Had the Sixth Circuit not quickly countered Simpson's illogical assault on the Act's privacy provisions, countless thousands if not millions of women in the 1970s and 1980's would have found themselves at the business end of a terrifying double barreled assault. At the time, society and the legal system was still turning a blind eye to psychical abuse in the domestic arena. *Simpson*'s widespread adoption by fellow circuits could have greatly added on their domestic control and victimization by having effectively legalized the practice of monitoring and recording their telephone calls—a relatively new phenomenon at the time made possible brought about by new technologies that allowed controlling spouses to monitor and record their telephone calls in order to continue their manipulation and control over them by freely intercepting their private phone conversations and using the recordings as blackmail and leverage against them in divorce proceedings.

[10] And just how bad was *Simpson?* Here is just a small sampl of reviewse; *United States v. Murdock,* 63 F.3d 1391, 1400 (6thCir. 1995) ("This court concludes that the absence of an interspousal exemption from the restrictions of Title III as recognized by this circuit, together with the general proposition that spying on one's spouse does not constitute use of an extension phone in the ordinary course of business, ..."), *cert. denied,* 517 U.S. 1187 (1996); *Glazner v. Glazner,* 347 F.3d 1212, 1215 (11thCir. 2003) (en banc) ("The language of Title III [18 U.S.C. §§ 2510–2522] is clear and unambiguous. It makes no distinction between married and unmarried persons or between spouses and strangers. **....** ... an overwhelming majority of the federal circuit and district courts, as well as state courts, addressing the issue have refused to imply an exception to Title III liability for interspousal wiretapping. [citing cases]"). Fifth Circuit However, in the Fifth Circuit (i.e., Texas, Louisiana, and Mississippi) spouses may wiretap each

Intent Under The ECPA

The MC confused the intent requirement in the ECPA. Tech touts its software as a means to "monitor a cheating spouse's computer without bringing undue attention." Indeed, the entire business model is based on WebWatcher's ability to surreptitiously intercept electronic communications. Operating through or on a third party device doe snot relieve a software designer of liability for intentionally intercepting communications. Like the software developer in In re Carrier IQ, Tech's conduct (developing and marketing WebWatcher) and the results achieved (intercepting Plaintiff's communications and routing them to its servers for storage) indicate intent.

In re Pharmatrak Inc. Privacy Litigation, 329 F.3d 9, 22-23 (1st Cir. 2003). In *In re Pharmatrak, Inc. Privacy Litigation*, the First Circuit remanded the case to the district court for determination of whether the defendant company intentionally violated 25 U.S.C. 2511(1)(a) of the ECPA. 329 F.3d 9, 22-23 (1st Cir. 2003). In discussing the meaning of the term "intentional" in the ECPA and in its legislative history, the First Circuit noted: Congress made clear that the purpose of the amendment was to underscore that inadvertent interceptions are not a basis for criminal or civil liability under the ECPA. An act is not intentional if it is the product of inadvertence or mistake. There is also authority suggesting that liability for intentionally engaging in prohibited conduct does not turn on an assessment of the merit of a party's motive. That is not to say motive is entirely irrelevant in assessing intent. An interception may be more likely to be intentional when it serves a party's selfinterest to engage in such conduct. 329 F.3d at 23. On remand the district court discussed whether a web-monitoring corporation's gathering of certain personal information of internet users for use by pharmaceutical

---

other, under the much criticized holding of *Simpson v. Simpson,* 490 F.2d 803, 805 (5thCir. 1974) ("However, we are of the opinion that Congress did not intend such a far-reaching result, one extending into areas normally left to states, those of the marital home and domestic conflicts."), *cert. den.,* 419 U.S. 897 (1974). *Simpson,* 490 F.2d at 806, n.7 also relied on interspousal tort immunity, a relic from the 1800s that is now rejected by most states in the USA.: *PV Intern. Corp. v. Turner,* 765 S.W.2d 455, 469-470 (Tex.App.-Dallas 1988) ("... we believe that the decision in *Simpson* is wrong. We, therefore, decline to follow it."), *writ denied,* 778 S.W.2d 865, 866 (Tex. 1989) (per curiam) ("The [Texas state] court of appeals declined to follow *Simpson v. Simpson,* 490 F.2d 803 (5thCir.), *cert. denied,* 419 U.S. 897, [...], which is factually analogous to the instant case."); *People v. Otto,* 831 P.2d 1178, 1185-1190 (Calif. 1992) (at 1188: "*Simpson's* reasoning has been subjected to severe criticism, and its holding has been repudiated by the vast majority of legal commentators and state and federal courts."); *Pollock v. Pollock,* 154 F.3d 601, 606, n.12 (6thCir. 1998) ("While the Fifth Circuit has not overruled that decision, it has been severely criticized by a number of other circuits, ...").

companies was intentional in violation of 25 U.S.C. 2511(a)(1) of the ECPA. In re Pharmatrak, Inc. Privacy Litigation, 292 F.Supp.2d 263 (D. Mass. 2003). The court analyzed whether the inadvertent transmission of users' personal information to the web-monitoring company's server constituted an "intentional interception" within the meaning of 18 U.S.C. 2511(a)(1):

A. The MC Ignored fact that WebWatcher is a type of automatic routing software

As properly explored in Councilman, the use of automatic routing software is a game changer when deciding whether or not an "intercept" occurred under the Wiretap Act.

> [U]nder the narrow reading of the Wiretap Act we adopt ., very few seizures of electronic communications from computers will constitute 'interceptions.' . 'Therefore, unless some type of automatic routing software is used (for example, a duplicate of all of an employee's messages are automatically sent to the employee's boss), interception of E-Mail within the prohibition of [the Wiretap Act] is virtually impossible.'

B. The MC Erred by Ignoring the Type of Acquisition Involved in this case and that Tech engaged in the violations during a protracted period of intercept.

Even if the narrowest interpretation of "interception" was properly used by the MC (which plaintiff believes it *was not*) the MC's ruling remains flawed if only because of the type of acquisition evidenced in this case. In a somewhat similar case, *Blumofe v. Pharmatrak, Inc*., 329 F.3d 9 (1st Cir. 2003), the court noted that the concept of a contemporaneity or real-time requirement, which evolved in other factual contexts, may not be apt to address issues involving the application of the Wiretap Act to electronic communications. *Id*. at * 21-22. The court also found that interception would be justified even under the contemporaneous standard of intercept when a program automatically duplicated part of the communication between an user and intended recipient, and sent the information to a third party. *Id.* Cases such as *Pharmatrak* still support this case even under the narrowest definition of intercept available. In this case, Tech's software, *Webwatcher*, acted much like a data logging program, but after the data was recorded, it then *also acted* as an automatic routing program since the user never had to do anything to send the acquired information to Awareness Tech's private servers thousands of miles away. So the program *itself* automatically sent the information.

> We then noted that Pharmatrak's program would qualify under the *Steiger* definition because it effectively was an automatic routing program. Id. Much like the data logging program there, the Procmail recipe file here acted as an automatic routing program. It analyzed all of the e-mails sent to Councilman's mail server in real time and copied the relevant ones while they were being delivered.
>
> – *US v. Councilman*, 373 F. 3d 197 (1st Circuit 2004)("*Councilman II*")

Thus, the acquisition of Plaintiff's data in this case mimics that found in *Pharmatrak* and the software used also automatically re-routed the acquired information. Therefore, the reasoning used by the Court in *Councilman* should be instructive to this Court as it surely will be to the appellate court in the coming appeal. Therefore, whether right or wrong about its acceptance of the narrowest reading of the already destructively narrow contemporaneous standard, Plaintiff retains standing because, as the Court in *Councilman* stated, "[e]ven those courts that narrowly read 'interception' would find that Pharmatrak's acquisition was an interception." *Id.* at 215.

The illegality of Awareness Tech's business model and its dangerous software should be obvious by now to anyone. This Court should finally recognize that illegal interceptions most assuredly happened here under *anyone's* definition of "contemporaneous" or their interpretation of "interception."

B. The MC Erred by Ignoring the Type of Acquisition Involved in this case

Even if the narrowest interpretation of "interception" was properly used by the MC (which plaintiff believes it *was not*) the MC's ruling remains flawed if only because of the type of acquisition evidenced in this case. In a somewhat similar case*, Blumofe v. Pharmatrak, Inc*., 329 F.3d 9 (1st Cir. 2003), the court noted that the concept of a contemporaneity or real-time requirement, which evolved in other factual contexts, may not be apt to address issues involving the application of the Wiretap Act to electronic communications. *Id*. at * 21-22. The court also found that interception would be justified even under the contemporaneous standard of intercept when a program automatically duplicated part of the communication between an user and intended recipient, and sent the information to a third party. *Id.* Cases such as *Pharmatrak* still support this case even under the narrowest definition of intercept available. In this case, Tech's software, *Webwatcher*, acted much like a data logging program, but after the data was recorded, it then *also acted* as an automatic routing program since the

user never had to do anything to send the acquired information to Awareness Tech's private servers thousands of miles away. So the program *itself* automatically sent the information.

> We then noted that Pharmatrak's program would qualify under the *Steiger* definition because it effectively was an automatic routing program. Id. Much like the data logging program there, the Procmail recipe file here acted as an automatic routing program. It analyzed all of the e-mails sent to Councilman's mail server in real time and copied the relevant ones while they were being delivered.
>
> – *US v. Councilman*, 373 F. 3d 197 (1st Circuit 2004)("*Councilman II*")

Thus, the acquisition of Plaintiff's data in this case mimics that found in *Pharmatrak* and the software used also automatically re-routed the acquired information. Therefore, the reasoning used by the Court in *Councilman* should be instructive to this Court as it surely will be to the appellate court in the coming appeal. Therefore, whether right or wrong about its acceptance of the narrowest reading of the already destructively narrow contemporaneous standard, Plaintiff retains standing because, as the Court in *Councilman* stated, "[e]ven those courts that narrowly read 'interception' would find that Pharmatrak's acquisition was an interception." *Id.* at 215.

Even more than emails, instant messages (IMs) reveal the weaknesses of the storage-transit dichotomy because IMs are "seldom saved" on the computer used to send or receive them, instead residing on a provider's internet servers. (R. 39, Compl. Pl.'s Ex. D2, PageID # 351.) IMs are not typically transmitted intact over dedicated circuits, but, like emails, are broken into "packets," sent over a network, and reassembled by the recipient's computer. *See Szymuszkiewicz,* 622 F.3d at 704–05; *Councilman*, 418 F. 3d at 69–70. Thus, when WebWatcher acquires IMs "in REAL TIME," as it claims on thousands of ads on the internet and has admitted to in this case, it acquires them in transient electronic storage . Electronic communications acquired while in transient electronic storage are intercepted contemporaneous with transmission because such storage is "part of the overall transmission process of an electronic message." *In re Carrier IQ*, 78 F.Supp. 3d at 1081. In *In re Carrier IQ*, plaintiffs challenged software on mobile devices that "surreptitiously intercepted personal data and communications and transmitted this data to Carrier IQ and its customers." *Id.* at 1058. The court drew a distinction between acquisitions of communications that "occurred after the transmission was completed" and the case before it, where the challenged software was "alleged to operate on sent and received communications

during the transmission process." *Id*. at 1078. The court found that, even if text messages "were in transitory storage on Plaintiff's mobile devices," the software could still intercept them "contemporaneous with their transmission." *Id*. at 1081. "[T]o hold otherwise would make the Wiretap Act turn on the intricacies of a particular circuitry's design: e.g. whether there is cache memory—an engineering intricacy that has no evident relationship to the purposes and policies of the Wiretap Act." *Id*. at 1081.

A. Various questions of fact remain in this case

In this lower forum, Tech never once raised any doubt or concerns about the advertisements submitted as exhibits pointing towards their illegal and illicit advertising strategy.

Tech did for the first time question them during appeals, wherein Plaintiff's representatives responded "Awareness cursorily disputes the validity of these exhibits for the first time on appeal …As a threshold matter, because Awareness did not challenge the validity of these exhibits below, it cannot do so on appeal." Awareness's implied arguments that these advertisements were not paid for or sponsored by Tech,[11] at most create questions of fact. Concerning Tech's previous affidavit, the Magistrate Judge correctly found that Mr. Miller's affidavit "is wholly silent regarding when WebWatcher forwards the recorded information to the secret account." (Doc.# 109 at *13) Again Plaintiff's representatives correctly replied, "Awareness did not object to this finding…. Accordingly, Awareness has waived its ability to challenge this finding on appeal."[12] Similarly in this lower forum, nothing Tech has submitted either to Plaintiff during discovery or to this Court clearly demonstrates that the actual functionalities of Web Watcher do not include a contemporaneous acquisition of electronic communications. This remains a question of fact. Moreover, as the MC noted in RR1, Plaintiff also alleged that Tech's "software did more than merely record keystrokes, because it also saves and/or records entire IM conversations and other 'screen' data. A portion of the recorded data originated from Plaintiff, from a remote computer on which WebWatcher was (presumably) not installed. The affidavit

[11] In appeals Tech also implied that the screenshots submitted within the exhibits were for a different spyware product called WebWatcher , or it was marketed by another company, or that it marketed WebWatcher differently when Mr. Zang purchased the product.

[12] Plaintiff is uncertain if the fact that Tech never objected or raised concerns about the exhibits within the first five years of this lawsuit, whether or not the issue is forever considered waived not only in that last appeal but in this lower forum, or if it is given new life upon reversal in appeals.

submitted by the CEO confirms that much broader data than keystrokes is captured by the spyware at issue." *Id.* Thus, Tech's own CEO confirmed that – like most similar rootkit based software - Webwatcher also takes screenshots at certain intervals. That *confessed* (or at least strongly implied) functionality alone adds to the remaining questions in this case and that extra ability has often been the difference maker in past decisions as to whether or not an "interception" has occurred in a case. While Webwatcher was not on Plaintiff's computer and thus not taking screenshots of his computer screen, it was taking screenshots on Catherine's screen (or it had the ability to do so) which was also displaying Plaintiff's private conversations in the opened IMs. The ability to take screenshots alone qualifies the mechanism as being capable of producing prohibited interceptions even under an interpretation of the FWA that requires interceptions of electronic communications to be contemporaneous with transmission. *See ex. Shefts v. Petrakis*, No. 10-CV-1104, 2012 WL 4049484, at *9 (C.D. Ill. Sept. 13, 2012) (finding that software that caused images of the plaintiff's email communications to be captured as they were being written and sent or received "contemporaneously captured Plaintiff's electronic communications within the meaning of the [FWA]"); *see also Potter*, 2007 WL 539534, at *6 (holding that "incoming emails subjected to the screen shot software" satisfy the FWA's definition of an interception of an electronic communication).[13] Moreover, any remaining dispute as to how WebWatcher works is a question of fact that the MC now seems to be feel has been resolved. With what evidence, Plaintiff remains unsure.

Significantly, acquisition of AP's communications was never even *challenged* by Tech as there was plenty of evidence available to prove it had done so. Thus, arguing arguendo, even if *somehow* Tech was properly found innocent of liability for the *intercepts*,[14] Tech's "use" and "disclosure" clearly violated the Act

---

[13] Tech violated the FWA's prohibition on using unlawfully intercepted electronic communications when it summarized his private messages when they acquired them on their servers . See 18 U.S.C. § 2511(1)(d). Tech also violated the FWA's disclosure provision by having sent them via email to Joseph Zang. See 18 U.S.C. § 2511(1)(c*); see also Noel v. Hall*, 568 F.3d 743, 751 (9th Cir. 2009) (holding

that 18 U.S.C. § 2511(1)(c) "protects against the dissemination of private communications that

have been unlawfully intercepted").

[14] An Intercept (§2511) was previously found to have occurred, and when it was the MC did not use any lax filing standards to get to that conclusion/recommendation. Rather it was a well reasoned and thought out exercise free of any standards outside of the right path to pursue in order to fulfill Congress; intentions when it authored the Act and then later updated it in the ECPA. The findings did not rely on any inferences or fact that are not present now. The messages were not acquired any quicker then. In its exploration the MC even noted that whether it was

because Tech did not challenge or address AP's claims (in the lower proceedings or in appeals concerning the following; 1) its advertising for illegal use was illegal, and 2) that they ***knew or should have known*** the illegal nature of the intercepts it was acquiring, using and disclosing. Therefore, Tech's summaries and deliveries given its undisputed ability (and/or duty) to know the illegal nature of the intercepts is a clear violation of 18 U.S.C §§2511(1)(c), (d).[15] This presents a problem for the SD because it never discussed whether Tech "knew or should have known" that the communications were being illegally acquired on its servers.[16]

The MC Erred In Finding Plaintiff's Expectations Of Privacy Was Inherently Diminished Due To A Lowered Expectation Of Privacy For The Married Victim In The Case.

The majority of courts that have examined the issue of intra-spousal privacy have held that spouses are no different than other individuals; spouses do not forfeit through marriage their expectation of privacy, even from one another. The cited cases apparently favored and endorsed by the MC are outdated and backwards looking cases that are in the minority that have all depended on *the absolute worst* circuit court decision in our lifetime; one so bad it's a somewhat of a laughing stock among the circuit courts. (see *Simpson* below). The MC has a long well objected to track record in this forum of building her case against Plaintiff with sketchy case law. (See Ex, XXX) This is perhaps the MC's crown jewel in the five long years Plaintiff has been in this lower forum.

Moreover, discussions or concerns about the ownership of the computer used in Ohio are of no consequence. First, even if ownership of the computer were relevant, it is a disputed fact that is for a trier of fact to decide; the jury. Nonetheless, contrary to the MC's assertion, WebWatcher was installed on a computer

---

instantaneous or within a blink of an eye, the proper standard was well reflected by the *Klumb* case. The MC dismissed thee case, but not because of this issue, which was ruled Plaintiff's way. Having been sent back, this ruling should have remained the same. Even if Tech acquires the communications from RAM, the milliseconds difference should not have caused such an improper and abrupt about face by the MC. Tech's actual acquisition of Plaintiff's messages violation alone, with or without liability later attaching, would have been enough for the purposes of enabling standing to sue under §2512, as it was a violation of §2511. Most courts recognize a cause of action for §2512 when in the presence of any violations of §2511.

[15] Throughout these proceedings, Tech never one denied nor did it address AP's claims that it knew or should have known the illegal nature of the intercepts it was acquiring, using and disclosing.

[16] In the first half of this case, only by having *somewhere* explored or denied that Tech could not have known the illegality of the communications–an impossibility given Tech's advanced capabilities and infrastructure – could the SD have properly found that Tech's use and delivery did not violate §2511, thereby negating reach of remedies for violation of §2512. Instead, the MC looked towards other variables not considered relevant to liability within the Act.

purchased during the marriage and is considered co-owned in the state of Ohio. Second, neither the federal Wiretap Act nor the Ohio statute provides an ownership exception to liability. See 18 U.S.C. § 2511(2)(d); Ohio Rev. Code Ann. § 2933.52(B)(4). The only stated exceptions are for interceptions made by a party to the communication or when such a party has consented to the interception. Id. Ohio law defines marital property to include "[a]ll real and personal property. . . owned by either or both of the spouses . . . that was acquired by either or both of the spouses during the marriage." Ohio Rev. Code Ann. § 3105.171(A)(3)(a)(i). Plaintiff can prove at trial that the computer was definitely purchased within two years of the start of the divorce proceedings. Catherine Zang would have attested to that at trial. Moreover, she kept the computer after the divorce because Mr. Zang barely knew how to turn the thing on, and needed his computer savvy sister to install Webwatcher for him. That is also in evidence within the records of this case (As noted by the MC in RRR on page 24, as well as in prior exhibits containing Jopseph Zang's testimony) as well as the divorce case which preceded this one. during "the period of time from the date of the marriage through the date of the final hearing in an action for divorce or in an action for legal separation," it was marital property to which both spouses had an equal claim of ownership. Ohio Rev. Code Ann. § 3105.171(A)(2)(a). Again, thisis a question of fact for a jury to decide and yet another issue where Plaintiff has shown that there do remains questions of fact in this case. This Court recognizes an expectation of privacy in emails sent through commercial internet providers. *United States v. Warshak,* 631 F.3d 266, 286, 288 (6th Cir. 2010). Plaintiff was "surely entitled to assume that his conversation [was] not being intercepted" without his consent regardless of who owned the computer used by the other party to his conversation. *See Katz v. United States*, 389 U.S. 347, 361 (1967) (discussing expectation of privacy in context of a public telephone booth and noting that "[t]he point is not that the booth is 'accessible to the public'

at other times . . . but that it is a temporarily private place whose momentary occupants' expectations of freedom from intrusion are recognized as reasonable"). A reasonable jury will easily find that Awareness illegally invaded Plaintiff's privacy. Intercepting electronic communications, such as email and IMs, constitutes an invasion of privacy under Ohio law. *Lazette v. Kulmatycki*, 949 F. Supp. 2d 748, 760–61 (N.D. Ohio 2013). Here, Awareness has submitted to Plaintiff during discovery evidence hundreds if not thousands

of intercepted Instant Messages revealing constant automatic surreptitious surveillance for at least a month and a half.[17] They were also submitted to Catherine Zang in the previously attached case. Awareness intercepted his "private communications" including "thousands" of emails and AOL IMs. Awareness knew or should have known its product would be used for just such invasions of privacy. Tech's argument that it had no viable link to the other defendants who allegedly disclosed his private communications" ignores the obvious. Had Awareness not intercepted Plaintiff's private communications and disclosed them to its customers, no other defendant could have accessed them. In other words, the initial intercept and disclosure was made by Awareness; the other defendants' use of the communications was derivative.

Privacy Was Invaded When Awareness Wrongfully And Repeatedly Intercepted His Conversations With Ms. Zang.

There is a strong connection between the Fourth Amendment prohibition against "unreasonable searches and seizures" (which regulates conduct of government agents who do not have a search warrant) and torts for invasion of privacy. A landmark U.S. Supreme Court case tells us: "... the Fourth Amendment protects people, not places." *Katz v. United States*, 389 U.S. 347, 351 (1967). Thirty-one years later, the U.S. Supreme Court clarified what it meant in Katz:

> But the extent to which the Fourth Amendment protects people may depend upon where those people are. We have held that "capacity to claim the protection of the Fourth Amendment depends ... upon whether the person who claims the protection of the Amendment has a legitimate expectation of privacy in the invaded place." *Rakas [v. Illinois*], [439 U.S. 128] at 143 [(1978)], ... See also *Rawlings v. Kentucky,* 448 U.S. 98, 106 ... (1980).

Minnesota v. Carter, 525 U.S. 83, (U.S. 1998).

Professor Orin Kerr has explained the concept concerning a similar case to the present one ;

> This case involves the continuous, ongoing surveillance of the contents of the Plaintiffs' incoming and outgoing electronic communications. Consistent with *Berger*, this Court should find that this conduct constitutes an "intercept" under the Wiretap Act. Any other holding will authorize warrantless that does not satisfy the requirements of *Berger*, which will create serious constitutional concerns.
>
> In *Berger*, the Supreme Court applied the Fourth Amendment where surveillance was performed as "a series [of intrusions] or a continuous surveillance" and not "one limited intrusion." 388 U.S. at 57. As a

[17] Given the illegal nature of the stolen communications, plaintiff could not admit them into evidence or submit them in a public filling.

> result, any statute that permits "a series or a continuous surveillance" must include rigorous privacy protections or may be facially invalid under the Fourth Amendment. *Id*. at 56; *Sibron v. New York*, 392 U.S. 40, 59-60 (1968) (noting that *Berger* struck down a New York statute setting forth a procedure for issuing wiretap warrants, but failing to include necessary safeguards to satisfy Fourth and Fourteenth Amendment scrutiny).
>
> Keeping in mind the relationship between *Berger* and the Wiretap Act, any ambiguity in the Wiretap Act's language should be construed consistently with *Berger*'s Fourth Amendment requirements. As a leading treatise on criminal procedure notes:
>
> Given the Wiretap Act's close connection to *Berger*, the meaning of "intercept" should mirror the distinction drawn by the Supreme Court in *Berger*. Acquisition is an intercept when it is part of "a series or a continuous surveillance," such as ongoing prospective surveillance or its functional equivalent. Exact lines will be difficult to draw, but the essential question should be whether the means of monitoring is the functional equivalent of continuous surveillance or whether it is more like a one-time or otherwise limited access to communications. LaFave, 2 CRIM. PROC. § 4.6(b).10

Similarly, this case involves the continuous, ongoing surveillance of the contents of the Plaintiffs' incoming and outgoing electronic communications. Consistent with *Berger*, this Court should find that this conduct constitutes an "intercept" under the Wiretap Act. Any other holding will authorize warrantless that does not satisfy the requirements of *Berger*, which will create serious constitutional concerns.

C. Licensing Agreement

The MC went on at length about the licensing agreement. (Doc.# 225 at p. 23-26). The MC seemed to believe that Tech's agreement showed the company had attempted to "protect the rights of victims similar to the Plaintiff, requiring purchasers to accept its licensing terms prior to being allowed to install its software." *Id*. At 26. The MC then again employed its typical use of questionable case law and selective interpretation by using the case of *Hayes v. SpectorSoft Corp.,* 2009 WL 3713284 (E.D. Tenn. Nov. 3, 2009) to support its findings, while ignoring the huge differences between the facts of these cases. Moreoever, the *Hayes* decision shows logical and internally inconsistency throughput the report.. *Hayes* at *5–6 (E.D. Tenn. Nov. 3, 2009). In *Hayes*, the court rested its analysis on the terms of the software's license agreement, which required customers to agree to "inform anyone who [sic] you may record that their Internet and PC activity is subject to being recorded and archived." Id. at *3. Based on this, the court found that the developer would be "unaware" that a person was "breaching the terms of its licensing agreement." Id. at *8. But the court dismissed an argument that the software should notify those being monitored because "[s]uch notices would reduce the efficacy of the legitimate uses for [the] software, such as employee and parental monitoring." Id. at

*8. The court said in one breath that the designer reasonably expected customers to inform subjects that they were being monitored and, in the next, that alerting subjects would "reduce the efficacy" of the software. This obvious inconsistency highlights the disingenuous nature of finding that a licensing agreement trumps the software's design in analyzing intent. Nothing in the record suggests that Tech expected its customers to inform those monitored that WebWatcher would surveil their communications. Nor would that expectation be reasonable given Tech's emphasis on WebWatcher's invisibility and design to "catch cheaters."

Further, concerning Ohio's product liability law, Plaintiff alleged Awareness owed the general public a duty to manufacture and maintain a safer product of intercept,[18] and its intentional failure to do so released a device of intercept into the stream of commerce, which device was the direct cause of Plaintiff's injury and loss. Web Watcher is certainly a "product" under the Wiretap Act. A reasonable jury would find that WebWatcher was unreasonably dangerous at the time it left the manufacturer, in that Awareness had not incorporated any reasonable safety measures into its design, and its advertising for illegal use left rendered its product particularly vulnerable–indeed *likely*–to be abused by the users its marketing campaign specifically targeted.

Awareness' blatant failure to mitigate the easily foreseeable misuse of its product, particularly in light of its active advertising for such use, enables both the end user and the corporation to continue to freely prey on our constitutionally protected communications. Reasonable steps to protect the public from illegal intercept of our private communications have never been taken by Awareness as such precautions would counter their aggressive business model—on that primarily relies on such thievery in order to remain atop the spyware industry in sales and monthly memberships. Moreover, Awareness' aggressive advertisements represent intentional misrepresentations strongly implying that the surreptitious recording of spouses or associates is legal, for if not, could they be *openly advertising* Web Watcher for such use? Coupled with Awareness' failure to incorporate reasonable, cheap and effective safety functions—such as the inclusion of pop-up banners

[18] While generally, a manufacturer of spyware software owes no duty to avoid emotional injury to the victim of the misuse of that software in violation of the software's licensing agreement, when a manufacturer markets a product for the specific purpose that caused the injury, it should be barred from later claiming that it owed no duty to those harmed by the use of the product in accordance to its marketing scheme.

informing users that their private conversations are being surreptitiously monitored—Awareness illegal business model continues to evidence a bold-faced effrontery for the laws of this land, and the constitutional protections afforded our private communications. Even to this day, Awareness continues to operate as *the absolute worst* offender within an already insidious and near monolithic world-wide corporate mechanism of private intercept that Congress never imagined would be allowed to exist due to the protections it intended in its drafting and amending of the Act. Thus, little imagination or further reasoning is needed for this Circuit to find that Awareness' role in the present action represents a gross and actionable negligence of the highest degree, and one it *must* be held accountable for in this action, if not under the Wiretap Act, then under suitable common or state provided laws. *Gootee v. Colt Industries, Inc.*, 712 F.2d 1057 (6th Cir. 1983)((reversing lower court's judgment of no cause of action, finding that there was sufficient evidence to send misrepresentation and negligence in design to the jury. Additionally, finding that in product liability action grounded in negligence, a manufacturer could be held liable if it failed to guard against dangers posed by foreseeable misuse).

I. Tech Should not be granted judgment on the section 2511 claims because There is no Contemporaneous Requirement Because the Act Prohibits Both The Interception of Electronic Communications in Transit as Well as Those in RAM or Temporary/Volatile Storage.

Although the Act/ ECPA's anti-interception provision does not in any way stipulate that "interception" of electronic communications must be contemporaneous with their transmission, subsequent circuit court case law, such as *Fraser v. Nationwide Mutual Insurance Co*. (352 F.3d 107, 113 [3rd Cir. 2003]), "has held that an 'intercept' under the ECPA must occur contemporaneously with transmission." However, other circuits have taken a more advanced approach, having either formally or informally adopted a broader approach to the intercept question that plaintiff believes is much more technically sound and constitutionally proper. In most of those cases the courts did not necessarily deviate or reject the standard recently adopted contemporaneous standard in this circuit – rather they simply recognized the full set and type of data meant to be protected by the Wiretap Act. In truth, a vast re-thinking of the contemporaneous standard –if not its rejection entirely– really *should be* explored in this case in order to right the many wrongs created by the

judicial system in its decades long "emasculation" of the Wiretap Act.[19] Nonetheless, in the alternative, a mere adjustment or tweak of the terms is all that is necessitated for now to get this case its proper day in court; a necessary and critical adjustment that will also protect hundreds of thousands of future victims (mostly female) whose ongoing abuse by their spouses is exponentially increased buy their spouses use of this maliciously designed and marketed spyware. In fact, aiding the already battered and abused was the original reason Plaintiff brought about this lawsuit in the first place back in 2011.

From the start and throughout this case, Plaintiff has argued against adoption of the narrow interpretation of the "contemporaneous" requirement of intercept, believing it has dangerously compromised the protection of our digital communications.[20] Plaintiff has previously advocated a case that more accurately dealt with the kind of advanced software used by most corporate peddlers of personal/employee monitoring spyware which affects hundreds of millions of employees and private citizens everyday.[21]

Regardless, the Sixth Circuit decided to adopt the dangerously narrow contemporaneous standard – ironically while reversing this Court's prior decision to terminate this case. Nonetheless, there remains critical wiggle room even within that disastrous standard if it must be observed. This Court should embrace the path to the more enlightened and constitutionally sound methodology as reflected in the more recent decisions of the First and Seventh Circuits.

A. Tech and the MC relied upon irrelevant or distinguishable case law that interprets a previous version of the Wiretap Act, which has since been amended.

---

[19] As just one example, in *Potter v. Havlicek*, 2007 U.S. Dist. LEXIS 19 10677 *11, Judge Rose opposed "a hyper-technical application of the contemporaneous requirement emasculating the ECPA."

[20] *See ex.*, Doc #: 91 in the 629 case, at * 6, filed on 10/12/12; *Luis v. Awareness*, Case: 14-3601 Doc. # 26 at *7

[21] That case, *Klumb v. Goan* was decided within this Circuit, and Plaintiff still believes the approach should be mimicked by this District Court as it likely represents the wave of the future in such cases. In *Klumb*, a man sued his ex-wife under the Federal Wiretap Act, 18 U.S.C. § 2520(b), and the Tennessee Wiretap Act, Tenn Code. Ann. § 39-13-603(a). At trial, defendant argued that no intercept had occurred because the software used, a keylogger identical to WebWatcher named eBlaster, did not "intercept" the communications as that term has been previously defined in the Wiretap Act. However, the court applied a "router switching analysis" finding that "a wiretap occurs when spyware automatically routes a copy of an email, which is sent through the internet, back through the internet to a third party's email address when the intended recipient opens the email for the first time." The court found "ample evidence" to show that a wiretap had occurred. *Klumb v. Goan* 100836 (E.D. Tenn. 2012).

Until recently, this Circuit had yet to rule on the contemporaneous requirement of intercept. However, in an appeal of this case, the Sixth Circuit did adopt that long problematic requirement, stating "We therefore hold that, in order for an 'intercept' to occur for purposes of the Wiretap Act, the electronic communication at issue must be acquired contemporaneously with the transmission of that communication*." Luis v. Zang*, 833 F. 3d 619, 627 (6th Cir. 2016). Therefore, for better or worse, the contemporaneous requirement is for now the accepted standard within this Circuit.

What matters most now is whether this Circuit will adopt the (plaintiff argues) outdated and "always technically wrong" narrow interpretation of that already overly narrow standard as adopted by the 3rd, 5th, 11th circuits – ancient and outdated rulings that were never technically correct, but that somehow have been adopted by the MC after it impressively rejected those approaches in its previous Report and Recommendation from 2013 ("RR1") (Doc. # 109 at p.*14) - or whether it will adopt the various broader approaches embraced by many state wiretap acts, some district courts within this same circuit, and sometimes evidenced within the appeals courts within the 1st, 7th, and 9th circuits; holistic legal approaches which plaintiff believes are much more enlightened as well as being constitutionally sound and technically proper. Moreover, none of those courts have rejected the "contemporaneous standard," and in fact the First Circuit has specifically accepted the contemporaneous standard but from a broader perspective than what has been evidenced in this case and in those technically improper and outdated decisions within the (mostly) southern circuits.[22]

This forum has battled Plaintiff in every single possible way for the past five year – and so it surely will be that *willing* American hero. Nonetheless, plaintiff at least needs to point out at this point that this Circuit can have its cake and eat it too. As shown by the First Circuit's ruling in *United States v. Councilman*, 418 F.3d 67 (1st Cir. 2005)(en banc), within that controversial contemporaneous standard lies some space for interpretation that allows a circuit to both accept the contemporaneous standard, and yet allow for a broader

[22] Plaintiff has previously stated (and recent world events have only confirmed) that the most backwards and despicable judicial decisions seem to emanate from the bowels of the country; aka the South (regarding the Act, such embarrassing, unconstitutional and technically flawed decisions as *Turk, Steve Jackson, Steiger, Simpson*). Its as if "Anti-lectuals" like Trump nominated everyone in those circuits. This is still a battle of North versus South in a way. It may always be that way. The Sixth should not follow those backwards circuits into the dystopian rabbit hole they want to drag us down into. The North is our only hope.

more enlightened approach that would allow for this case to proceed to trial ; one similar to the approach this same Court advocated so eloquently in 2013. The differences between the circuits are critical distinctions that can help mold our digital privacy protections for many years to come. While the District Court is perhaps not a forum that can by itself change the operating standard in this circuit, it could nonetheless advocate the more sophisticated and technically correct approach with its rejection of the MC's oddly new regressive approach to a matter it had once advocated rather well. To help reach that decision, this Court should reconsider the plethora of outdated circuit decisions that the 3rd, 5th, and 11th have used as the foundation for their contemporaneous arguments; one that requires a different treatment of electronic communications/emails in storage than those in transit. As previously discussed, that distinction is not supported by the Act nor is it found within its plain language. Congress never excluded electronically stored information from electronic communications, but it did from wire and oral communications.

B. The Wiretap Act's plain language makes no distinction between electronic communications in transit and those in electronic storage.

Nowhere in the Federal Wiretap Act does it state that an electronic communication cannot be intercepted while it is in storage. In fact, the Wiretap Act never mentions "electronic storage" in any of its relevant provisions. Tech and the MC would have this Court believe that the Act creates a dichotomy between electronic communications in transit and electronic communications in storage and that the Act only protects the former from interception. This is plainly untrue. The Act treats electronic communications in transit and in storage identically.

The plain language of the Wiretap Act never states that electronic communications can only be intercepted simultaneously with their transmission. The Act applies to "wire communications," "oral communications," and "electronic communications"; each of these three communications are treated differently under the Act. 18 USC § 2511(1)(a) (LEXIS 2015). The Act's own language limits wire communications and oral communications to contemporaneous interceptions, but refuses to extend such an interpretation to electronic communications.

B. The Plain Language of the Wiretap Act Does Not Require A Contemporaneous Requirement and Congress Defines Intercept To Include Acquisitions, Which Need Not Be Contemporaneous Under Any Standard.

By the Act's plain language, canons of construction, and the legislative history of the Act, it is obvious that Congress did not intend for electronic communications in storage to fall beyond the purview of the Act, and that to do so would produce an absurd result in the interpretation of the Acts protections. Such an approach is supported by the reasoning used in *Councilman*, as follows.

> The district court seemed to agree with one predicate of the Government's argument when it acknowledged that "technology has, to some extent, overtaken language" and that "[t]raveling the Internet, electronic communications are often— perhaps constantly both `in transit' and `in storage' simultaneously." *Councilman*, 245 F. Supp. 2d at 321. This apt observation should have prompted a different legal conclusion.
>
> All digital transmissions must be stored in RAM or on hard drives while they are being processed by computers during transmission. Every computer that forwards the packets that comprise an e-mail message must store those packets in memory while it reads their addresses… Since this type of storage is a fundamental part of the transmission process, attempting to separate all storage from transmission makes no sense.

This Court should find the more recent string of cases that apply the Act to electronic communications in storage more persuasive than those of the outdated cases relied upon by the circuits that adopted the narrower interpretation; cases that rely on a version of the Act that has since been amended.

Unlike with wire communications, Congress did not restrict electronic communications to communications in flight. Congress chose to omit wire communication's requirement of "between the point of origin and the point of reception" from the definition of electronic communications. *Id.* § 2510(12). Congress also chose to replace wire communication's "aural transfer," which requires the transfer to be "at any point between and including the point of origin and the point of reception," with electronic communication's "any transfer." *Id.* § 2510(18); § 2510(12)(emphasis added). To ensure that there is no confusion, Congress specifically stated that electronic communications exclude wire and oral communications. *Id.* § 2510(12) If Congress intended to include a contemporaneous requirement as to electronic communications, it would have included the contemporaneous language it included in wire communication and aural transfer. Where Congress includes particular language in one section of a statute but omits it in another section of the Act, it is generally presumed that Congress acts intentionally and purposely in the disparate inclusion or exclusion. *Russello v.*

United States, 46 U.S. 16, 23 (1983). Furthermore, Congress specifically enumerated four exceptions to electronic communications, one of which had to do with a certain type of electronically stored information. *Id.* § 2510(12). If Congress wanted to exclude all stored electronic communication from the Wiretap Act, it would have done so here. Where Congress explicitly enumerates certain exceptions to a general prohibition, additional exceptions are not to be implied in the absence of evidence of a contrary legislative intent. *TRW v. Andrews*, 534 U.S. 19, 28 (2001); *Councilman,* 418 F.3d 67, 75 (rejecting Defendant's argument that Congress intended to exclude stored electronic information from electronic communications because if Congress wanted to do so it would have included it as a numerated exception to electronic communications).

In fact, the only purported support whatsoever contained within the four corners of the Act is the ordinary usage meaning of intercept, which may suffice in football but is useless to address the nuances of an email's transfer throughout the web. *United States v. Szymuszkiewicz*, 622 F.3d 701, 705 (7th Cir. 2010). However, Congress chose to define intercept instead of relying on its ordinary usage meaning by defining it as "the aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device." *Id.* § 2510(4) (emphasis added). If Congress wished, it easily could have added its contemporaneous requirement in wire communications and aural transfer into its definition of intercept. *Wesley College v. Pitts*, 974 F. Supp. 375, 386 (D. Del. 1997) (agreeing that Congress could have added the language if it intended a contemporaneous requirement, but rejecting that argument in favor of an argument based on a textual contradiction, which, as noted below, Congress has since corrected). Not only did Congress not apply its contemporaneous language from terms defined before and after intercept, but Congress added the key language of or other acquisition to ensure intercept need not be contemporaneous. *Id.* § 2510(4).

Acquisition's plain meaning is to acquire or gain—contemporaneous is not an element of acquisition, regardless of the usage. Congress did not intend a contemporaneous requirement because it defines intercept to include the acquisition of emails.

C. Plain Language Aside, The Legislative History And Policy Considerations Also Support Interpreting The Act To Equally Protect Electronic Communications In Transit And Those In Storage.

Congress did not intend a contemporaneous requirement for at least three primary reasons, as follows; (1) because Congress' goal was to expand the protection of electronic communications not limit protections, and (2) a congressional report that Congress relied on explicitly stated that emails could be intercepted in storage after transmission, and finally, (3) Interpreting the Wiretap Act without reading in a contemporaneous element was Congress' intent when it wrote the Wiretap Act and then later expanded it with its later passing of the The Electronic Communications Privacy Act of 1985 (ECPA).

The ECPA was passed in the mid 1980s because the advent of electronic communications at the beginning of the decade (principally email) suggested to many that the Wiretap Act needed revision. *Councilman*, 418 F.3d 67at p.*76. Thus the ECPA was introduced to amend the Act to incorporate electronic communications—largely emails (and later instant messaging). *Id.* Shortly after the bill was introduced, the Congressional Office of Technology Assessment released a study of the privacy implications of electronic surveillance *Id.*;[23] The Report listed five stages at which an email could be intercepted. *Id.* (emphasis added). The stages at which interception could occur included "in the electronic mailbox of the receiver, when printed into hardcopy, and when retained in the files of the electronic mail company for administrative purposes." *Id.* at 48. The Report went on to note that existing law offers little protection and emphasized that "interception of electronic mail at any stage involves a high level of intrusiveness and a significant threat to civil liberties." *Id.* at 48, 50 (emphasis added). Congress passed the bill based on this study and against the Department of Justice's wishes, which wanted to give less protection to electronic communications. *Councilman*, 418 F.3d at 76-77.

[23] See Office of Technology Assessment, Federal Government Information Technology: Electronic Surveillance and Civil Liberties, available at http://www.wws.princeton.edu/ota/disk2/1985/8509_n.html (Oct.1985) ("Report").

Congress did not intend a contemporaneous requirement because the congressional report Congress relied on explicitly stated that emails could be intercepted in storage after transmission and because Congress' goal was to expand the protection of electronic communications. A contemporaneous requirement would nearly remove emails from the purview of the Act because emails are actually in flight for only a short period of time. There is only a narrow window during which a contemporaneous email interception may occur—the seconds or milliseconds before which a newly composed message is saved to a temporary location following a send command. *United States v. Steiger*, 318 F.3d 1039, 1050 (11th Cir. 2003). Unless an email is intercepted in that split second, Defendants' reading of the Act effectively makes it impossible for email interceptions to violate the act. *Id.* Furthermore, the Act itself defines electronic storage to include any temporary or intermediate storage of an electronic communication. *Id.* § 2510(17). Because emails are consistently in intermediate storage as they travel through the internet, and because Congress plainly stated even intermediate storage counts as storage, Defendants' contemporaneous argument would effectively remove all emails from the purview of the Act. This is an especially absurd conclusion as one of the amendment's primary goals was the protection of emails. Congress intended the broad definition of electronic storage to offer broad protection to stored communications, not to exclude them entirely from the purview of the Act. *Councilman*, 418 F.3d at 77-78 (Congress sought to ensure communications in pre- and post-transmission storage were protected. Congress, responding to the Report's concerns, sought to ensure that messages "stored in a user's mailbox are protected from unauthorized access"). This is why *Councilman* and its progeny resort to legal acrobatics to piece together a contorted reading under which there is a contemporaneous requirement but one that does not always apply to all communications in storage. *Councilman*, 418 F.3d at 79. The more straightforward approach is consistent with Congress's intent and the Act's plain language—the Act does not distinguish between electronic communications in storage and in transit.

The modern trend in case law and Congress' intent require construing the Wiretap Act without a contemporaneous requirement.

As set forth below, the recent trend in case law is that a distinction between electronic communications in transit and in storage is unrealistic and problematic. The recent trend, to eliminate the storage/transit dichotomy, applies the better reasoned, more practical approach than the string of outdated

cases that Defendants rely on. In *Potter*, a more recent case than those cited by Defendants, the Southern District of Ohio presented a more reasonable reading of the Wiretap Act when it found the Act did not require a contemporaneous element. *Potter v. Havlicek*, 2007 U.S. Dist. LEXIS 10677, *19 (S.D. Oh. Feb. 14, 2007). In *Potter*, the plaintiff sought injunctive relief to bar further disclosure when her emails with another person were intercepted by a third party. *Id.* at *2. In her motion for injunctive relief, she alleged that the third-party accessed the recipient's email accounts by secretly obtaining her password without permission and later disclosed the emails to others, including neighbors, friends, business associates, and the third-party's lawyer. *Id.* at *2-3. In ruling on the merits of the case, the court refused to follow other circuits' "hyper-technical application of the contemporaneous requirement" in the Wiretap Act and instead found that the emails did not need to be intercepted contemporaneously. *Id.* at *18.

The *Potter* court found merit in Judge Reinhardt's concurring and dissentingopinion in *Konop v. Hawaiian Airlines, Inc.*, 302 F.3d 868, 886 (9th Cir. 2002). *Id.* at 18.The *Potter* court also found merit in *Councilman*, 418 F.3d 67. There, the First Circuit determined that the contemporaneous requirement, which had been inserted by earlier courts, was not a requirement under a proper interpretation of the Wiretap Act and upheld Mr. Councilman's conviction. *Id.* at 78-9. *Councilman* represents the more logical, well-reasoned, and proper analysis of the "contemporaneous" requirement than *Councilman* was also an *en banc* opinion of the First Circuit. In *Councilman*, the First Circuit reversed the lower court's dismissal ofCouncilman's indictment because the lower court improperly relied on the second *Konop* decision to read a contemporaneous requirement into the act. *Id.* at 71. Councilman was indicted for directing its server to intercept and copy email messages passing through its servers from Amazon.com to Councilman's customers. *Id.* at 70. Councilman's interception occurred only while the e-mails were in storage on Councilman's computer. *Id.* at 71. The court in *Councilman* analyzed the Wiretap's plain language and legislative history and, for the reasons stated supra, found that Congress amended the Act to offer greater protection to emails located in storage—not to exclude them from the Act's protection. *Id.* at 72-79. There can be no contemporaneous requirement because Congress drafted the Act to protect emails in

storage.

Although the First Circuit in *Blumofe* did not need to rule on the existence of a contemporaneous requirement, it noted that it shares the concern of the Ninth and Eleventh Circuits about the judicial interpretation of a statute written prior to the widespread usage of the internet and World Wide Web in a case involving purported interceptions of online communications. *Blumofe v. Pharmatrak, Inc.* (*In re Pharmatrak, Inc. Privacy Litig.),* 329 F.3d 9, 21 (1st Cir. 2003) (Citation Omitted). The court noted: "In particular, the storage-transit dichotomy adopted by earlier courts may be less than apt to address current problems." *Id.* This Court should also find the *Hall* opinion instructive, in which the Second Circuit rejected the argument that "communication over the Internet can only be electronic communication while it is in transit, not while it is in electronic storage." *Hall v. EarchLink Network, Inc.,* 396 F.3d 500, 503 n.1 (2d Cir. 2005).

The Wiretap Act contains three different "Titles." Only the first two, Title I and Title II, are of relevance in this appeal. Generally speaking, Title I is implicated with the use of the spyware used in this case, and Title II is implicated when one hacks into another's email account FIX THIS. More specifically, Title II created the SCA to cover access to stored communications and records, and generally prohibits access to stored information on a server or computer. Unlike Title I,[24] the SCA applies only to stored communications. *See* 18 U.S.C. §2701(a); *Konop v. Hawaiian Airlines, Inc.,* 302 F.3d 868, 874 (9th Cir. 2002). Of primary concern in this appeal, the SCA creates criminal and civil penalties against whoever "intentionally accesses without authorization a facility through which an electronic communication service is provided." 18 U.S.C. §§2701(a)(1). "Electronic communication service" is defined as "any service which provides users thereof the ability to send or receive wire or electronic communications." 18 U.S.C.§ 2510(15). Any company or government entity that provides others with the means to communicate electronically can be a "provider of electronic communication service" relating to the communications it provides, regardless of the entity's primary business or function. *See Fraser v. Nationwide Mut. Ins. Co. , 352* F.3d 107, 114-15 (3d Cir. 2004) (insurance company that provided email service to employees is an ECS). Appellee can be seen as providing its users the ability to send or receive electronic

[24] The terms "Title I", Wiretap Act," and "ECPA" are often used interchangeably in the legal arena. The ECPA was an amendment to Title III of the Omnibus Crime Control And Safe Streets Act ('OCCSSA'). Further confusing matters, OCCSSA itself is also known as "the Wiretap Statute." For the sake of clarity within this section, Title I will only apply to

communications both to its servers, and from its servers to whatever computer or device they send or retrieve the stored messages.

Significantly, the SCA it is not limited to unlawful access to a computer or facility alone. Instead it also prohibits such access to a *network* without authorization. Therein lies a mildly complicated concept relevant to Appellant's SCA claims. At the time of the alleged violations of the Act by Tech, Appellant used various Internet Service Providers ('ISPs'), such as America Online ('AOL"), Yahoo, and Gmail to both send and receive emails and instant messages. All of the above ISPs are considered ECS as defined in the SCA. The majority of the relevant communications rerouted by Web Watcher onto Tech' private servers were obtained somewhere within a temporary amalgam of purpose created within cyberspace. This practically indefinable union of personal devices and infrastructure represented a communications tunnel or perhaps cubicle—practically a high tech virtual phone booth—carrying and temporarily hosting constitutionally protected communications. The tunnel is formed by a technically complex interaction between 1) Appellant's personal computer, 2) the privately owned servers and software of AOL,[25] 3) the Internet's publically accessible infrastructure, and 4) the computer of the intended recipient of Appellant's communications, Ms Zang, who Appellant believes also primarily depended on those three ISP's for her Internet-based electronic communications. In addition to intercepting every single message both to and from Ms. Zang's computer, Web Watcher also recorded all of her browsing history and took snapshots of websites visited, as well as snapshots of instant message sessions, along with the intercept of those messages themselves. Obviously Web Watcher violated all aspects of the Wiretap Act concerning Ms. Zang. The question remains, what aspect did it violate against Appellant in this case? Firstly, a large volume of Instant message and emails originating from her computer in Ohio were inevitably re-routed onto Tech' own servers, summarized ('used') and delivered by Tech prior to Appellant having either received, or read those emails. Depending on the standards applied to such interceptions during a court's interpretation of the Act, those intercepts represent either a violation of the Act, or the SCA. Due to the way that the Internet works, and how information packets travel to and from many different servers, instead of directly to their intended recipients,

[25] For the sake of simplicity, Appellant will use "AOL" to represent all of those ISPs during the rest of this discussion, for both his own use and Ms. Zang's. .

courts applying the narrow interpretation of "intercept" have often ruled that such communications were not intercepted, but merely retrieved from temporary storage. In fact, for decades, small time hackers as well as larger entities of intercept–both public and private–have successfully depended on such a narrow interpretation by the judiciary in order to relieve themselves of liability under the Act. As far as Appellant knows, as he was effectively denied Discovery against Tech, Web Watcher was only installed on the Ohio computer.[26] The statute defines "intercept" as: "any temporary, immediate storage of wire or electronic communications incidental to the electronic transmission thereof." The communications originating from Appellant's home in Florida were first sent to AOL, where they resided in temporary storage before AOL created a virtual tunnel within the Internet itself, wherein Appellants AOL account is temporarily "consolidated" with Ms. Zang's AOL account, opening a gateway between the two computers wherein the packets of information travelled on their way to and from Ohio. Prior to the communication reaching Ms. Zang's computer, where they would then be placed into temporary storage in some manner; likely the RAM.[27] Web Watcher then copied the information in a blink of an eye and either sent it immediately or funneled it onto her hard drive until the communication was over, wherein tech claims WebWatcher then transmitted a copy of the communications to Tech' personal servers, apparently somewhere in California. Thus the intercept or illegal access to the privileged communications did not physically occur on Appellant's computer, nor did they need to have been so accessed. Web Watcher may not have resided on his own computer hard drive, yet when Appellant sent communications towards the infected computer, it was surely accessing his communications somewhere within the tunnel created between his computer, AOL,[28] the Internet, and Ms. Zang's computer. That ineffable tunnel is rightly seen as an extension of all four of the entities involved. And yet in truth, there were five entities in that tunnel. However, one of those

---

[26]

[27] Although during its early years, AOL was used primarily from the desktop, and was not Internet based, the service began to mimic GMAIL and other such ISPs, in order to compete with those providers. in its earliTitle II does not protect communications on a person's hard drive. Emails sent or received on AOL would typically be stored as a file on AOL's servers both prior and after their access by Appellant, or Ms. Zang—although in the case of a desktop client, they could be automatically saved on the hard drive, or of course downloaded from there to the hard drive. but such a practice is rare as they remain better protected on the ISP's servers. In the case of instant messages, the communications were placed within AOL's shared cache on her hard drive. Nonetheless, as stated above, Web Watcher intercepted and re-routed the communications prior to their placement on the hard drive, when they remained in "electronic storage."

[28] Because AOL is fully considered an ECS under the Act, improper access by Tech' mechanism of intercept, which effectively reached into the tunnel created by AOL is relevant to Appellant's SCA claims.

entities is not like the other. The uninvited outlier in this instance was, of course, Tech Technologies, whose advanced software, Web Watcher, operated as a kind of long armed "spike Mike;" an agent and extension of that company during the entire period of illegal intercepts. In effect, Web Watcher can be seen as having improperly accessed and obtained Appellants stored communications travelling within an extension of an ECS in violation of the SCA. Of course the same is applicable to messages being sent to Appellant.

Cases like the present will one day be considered important if we want to stave off a new digital dark age where everything and everyone can intercept and spy on us electronically without us having any reasonable recourse. As we tweet and like and upvote our way through social media, Americans generate a vast trove of data on what they think and how they respond to ideas and arguments. *Inside Russia's Social Media War On America*, Massimo Calabresi | Time Magazine. Thu, 18 May 2017.[29] All of those digitized convictions are collected and stored, and much of that data is available commercially to anyone with sufficient computing power to take advantage of it. *Id.* The Russians used this to their advantage in influencing this election, and many other avenues of manipulation remain available to countless malevolent entities. Without judicial interference in bolstering the Act's intended prongs of protection, our privacy in the Digital Age is all but forever doomed. This particular Court has been painfully slow to recognize the importance of helping to shut off some of those open portals to corporate and dictatorial domination. Instead of presenting this Plaintiff with further unnecessary roadblocks, this Court should help fight the fated rise of technically oriented corporate oligarchies that have recently become greatly empowered by greedy politicians now in office. Adding to the urgency, those interests want to leverage our digital privacy to benefit their bottom lines while increasing their leverage and political power. Combined with the hard-right radical political climate in which we now find ourselves, justice and Democracy *itself* requires this Court rise to the occasion and help bolster our digital privacy rights. As such, it should reject some if not all of the Magistrate's recommendations.

Finally the MC abused discretion by not accepting the attempted amendments, or using them in her reasoning. Given the many elements stated above, this Court should reconsider and/or accept the previously

[29] *See ex*, http://time.com/4783932/inside-russia-social-media-war-america/?xid=homepage&pcd=hp-magmod

tendered amendment as fully accepted by this Court. Additionally, this Court should now help this case bolster our digital privacy protections by assigning local counsel. This case the consideration, and our privacy rights demand it. Lastly, this Court should wait to rule on the magistrate's recommendation until the end of Discovery – a deadline that Tech itself has indicated by email that it intends to extend. (Exhibit K) This will allow Plaintiff a chance to further amend if he finds it necessary to do so given any new or critical information. Alternatively, this Court should allow leave to further amend to clear any deficiencies.

.

Dated: May 11, 2014

Respectfully Submitted,
/s/ Javier Luis
Javier Luis, *Pro Se*
jdluisohio@gmail.com

CERTIFICATE OF SERVICE

I certify that a copy of the foregoing Objection was filed electronically on May 11, 2014. Parties may access this document through that system.

/s/ Javier Luis Pro Se